Data retention:
The Belgian Experience

HLEG – Adèle

Head of DGJ-DSU-NTSU

Brussel 21 th 11 2023

NTSU DSU

Police Fédérale
Federale Politie

Data retention : a complicated story

- 2006 : 1st Belgian law on data retention
- 2015 : Law annulled by the Belgian Constitutional Court
- 2016 : New law on data retention with restriction on the acces to the data for the law enforcement
- **2019 :** New appeal for annulment against Data Retention
- **06/10/2020 :** Ruling of the European Court of Justice (ECJ) (Quadrature du net)
- **22/04/2021** : Belgian Constitutional Court made a “Copy-paste” of the decision CEJ
- STARTED AT THE NEW LAW

Federal Police

Despite this long « Story »!

Some authorities doubt whether data retention is really still needed for « a Modern LEA » in 2021

Police Fédérale
Federale Politie

FIRST STEP

Arguments for maintaining a minimal data Retention in Belgium

Federale Politie
Police Fédérale

1

The figures – Amount of data needed

Federale Politie
Police Fédérale

Some figures

	2021	Comments
Identifications RMS (on Nr)- TANQ	More than 1.628.000	Data retention
Network observation	12.246	Data retention
Retro observation	38.205	Data retention
Technologies	IP – 3G – 4G LTE/WiMax – IMS - Volte VoWifi et 5G	
GAFAM – SPOC OTT	8.597	Data retention & E-Evidence
Centralized wired tapping	10.744	No Sky-ECC without data retention

Source: NTSU

Federal Police

DATA RETENTION

= Fuel for Justice and Police work

NO investigation against organised crime without D.R.

e.g. sky ECC

Federal Police

2

And without Data retention ?

Federale Politie
Police Fédérale

Perverse effects in criminal investigation?

What if data retention disappears?

Loss of efficiency (much more means, more time, ...) to achieve (or not) a result

Federal Police

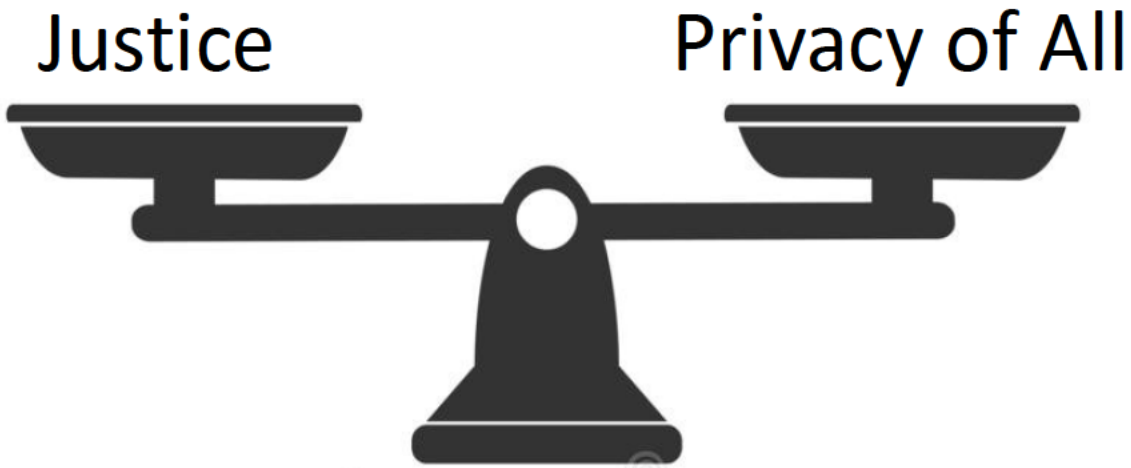
Perverse effects?

Mandatory use of more intrusive alternatives :

- Interception, tapping (e.g.: worrying disappearance of a person (abducted?)
- Physical observation according to the 'BOM' Act.
- Covert search
- Data collection by the law enforcement services instead of the operators.

For supposedly more privacy → there is a great risk of more intrusion in the people's privacy

The classical (incorrect) Balance



What about the commercial interests of enterprises – Are the LEA a less trusted party than private cie?

Federal Police

Some topics seem to be forgotten in the debate

Federale Politie
Police Fédérale

Forgotten in the debates

Protection of the « normal » citizen	**Endangered missing person** **Per year : 1.500.** **Young people who commit suicide : 1265**
Protection of the consumer	**Has the right to contest an invoice, or be helped when he is a victim of stalking, fraud, etc.**

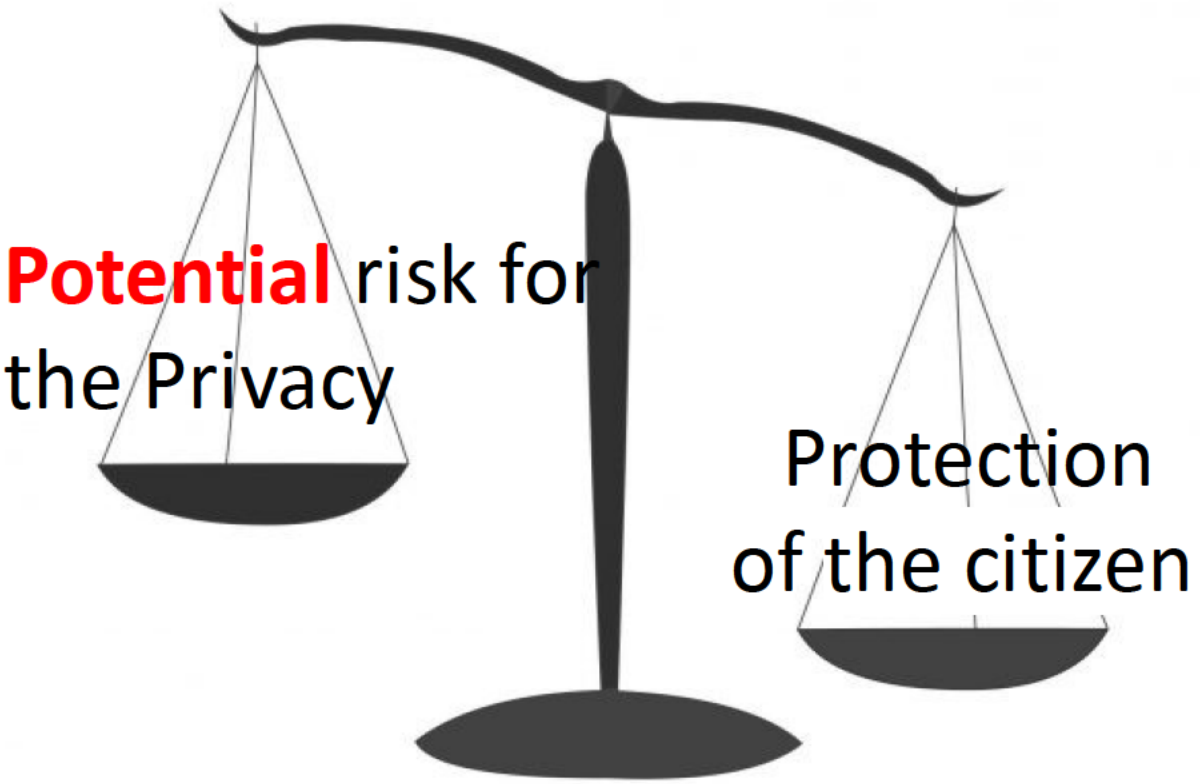
Forgotten in the debates

Protection of the network (NIS)	How can an operator achieve this without a minimum of data.
Protection of the victims	Avoid potential victims, legitimate right for the victim to have a protection from the State.

Forgotten in the debates

Privacy of the suspects	D.R. is one of the first means used to exclude a large number of potential suspects from our investigations They go from being “**suspects**” to being "**not involved**".
Proportionality of the measure	Without D.R. the law enforcment will be obliged to use other, more intrusive means to investigate.

The real balance to find is the following



Commercial interests of the Cie and entreprise – Advertising

Thanks to this « Narrative » decision was made to repair **again** the Belgian law

Federal Police

Principles of the New belgian law. How did we build the law ?

Federale Politie
Police Fédérale

Method

Federal Police

Proposal : *Lasagne*

Provide a succession of specific proportional – and differentiated - criteria that legitimize the retention of data

Each one has is own :

- Justification
- Duration
- Type of data that has to be kept

Federal Police

Result : 22/07/2022

Federale Politie
Police Fédérale

Layers of belgian data retention

Purpose	Data	Retention period
Basic subscriber Identification	Identification data IP address used for subscription	As long as the electronic communications service is used and 12 months after termination of service
	IP address used for communication Identifier of end device	12 months after end of session
	MAC-address	6 months after end of session
	Other identifiers (determined by the King)	Period determined by the King, but can not exceed 12 months
Their own data	Needed for the Cie T.O.R.	GDPR

Layers of belgian data retention

Purpose	Data	Retention period
Protection of the consumer right (prevention of Fraud)	Identifier at source & destination Date & time of communication	4 months following the date of communication
	Phone number at the source of incoming communication IP address, used port Date & time of communication	12 months following the date of communication
	Localization data for fraud prevention	Max. 4 months

Federal Police

Layers of belgian data retention

Purpose	Data	Retention period
Protection of the consumer right (prevention of Fraud)	Identifier at source & destination Date & time of communication	4 months following the date of communication
	Phone number at the source of incoming communication IP address, used port Date & time of communication	12 months following the date of communication
	Localization data for fraud prevention	Max. 4 months
Security of their Network	Security related traffic and localization data	Max. 12 months

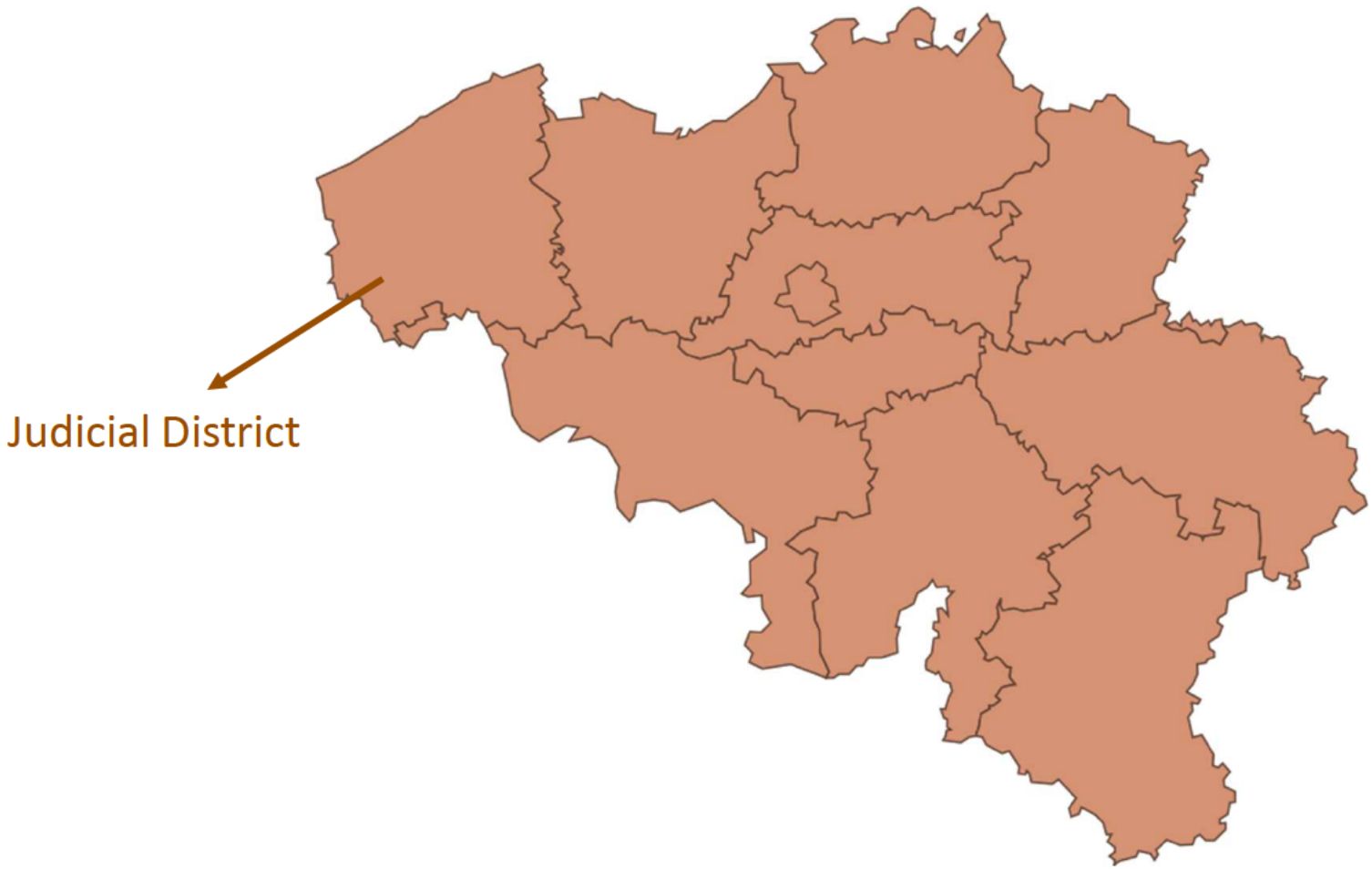
Federal Police

Layers of belgian data retention

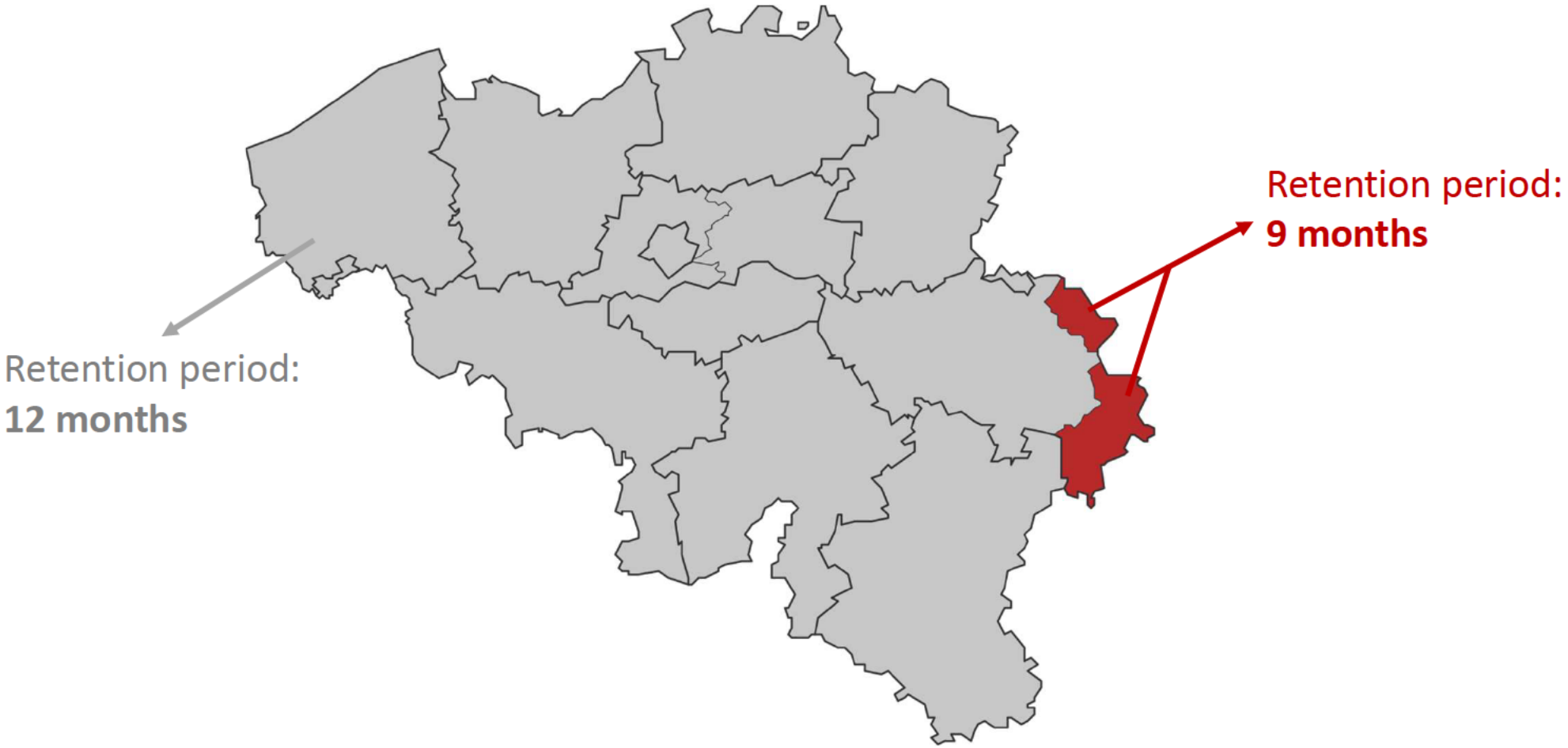
Purpose	Type of data	Retention period
Areas particularly exposed for the perpetration of serious crime (Geographical zones)	Identification & Traffic data	6, 9 or 12 months, determined per Judicial District or Police Zone. Determined by statistics based on crime rates (4 – 6 - > 7 crimes/1000 – mean on 3 years)

Federal Police

Geographical zones



Geographical zones 22-23



Layers of belgian data retention

Purpose	Type of data	Retention period
Areas particularly exposed for the perpetration of serious crime (Geographical zones)	Identification & Traffic data	6, 9 or 12 months, determined per Judicial District or Police Zone. Determined by statistics based on crime rates (4 – 6 - > 7 crimes/1000 – mean on 3 years)
Areas particularly exposed to threats against national security	Identification & Traffic data	For the duration of the threat **When the level of the threat reaches level ≥ 3** = determined by the Coordination Unit for Threat Analysis (CUTA)

Federal Police

Attack Brussels 16/10/2023

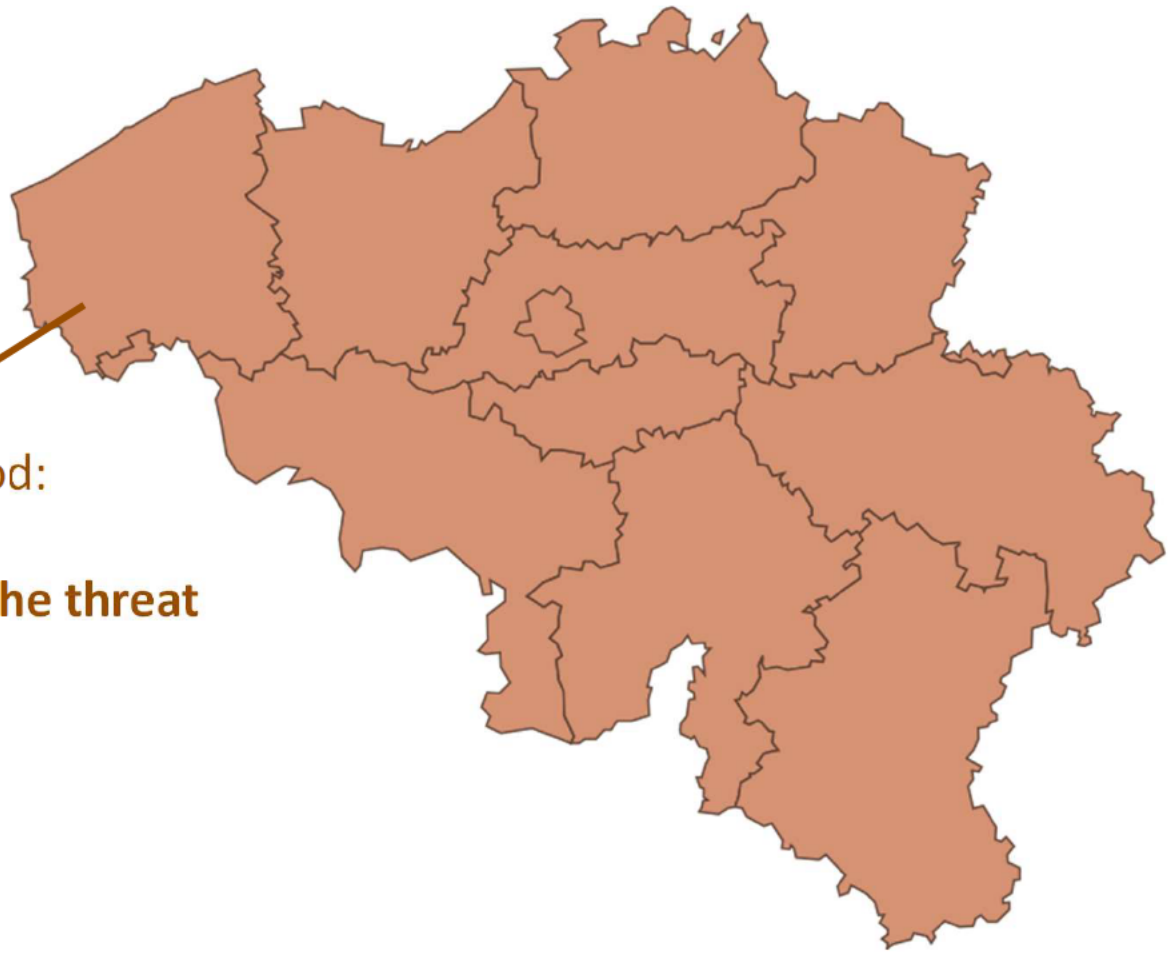
A new Terror attack occurred in Brussels on Monday evening.

Base on this fact and the analyze of available intelligence, CUTA (OCAM in Franch) raised the threat level against the national security in Belgium to level 3 – on the all territory - , meaning the threat is serious.

NTSU informed all service providers that they had to preserve their data – general and undifferentiated – for as long as the threat level persists.

This decision was confirmed by royal decree (17/11/23).

Geographical zones – Threat level ≥3



Retention period:
National,
For as long as the threat level persists

Layers of belgian data retention

Purpose	Type of data	Retention period
Areas particularly exposed for the perpetration of serious crime (Geographical zones)	Identification & Traffic data	6, 9 or 12 months, determined per Judicial District or Police Zone. Determined by statistics based on crime rates (4 – 6 - > 7 crimes/1000 – mean on 3 years)
Areas particularly exposed to threats against national security	Identification & Traffic data	For the duration of the threat **When the level of the threat reaches level ≥ 3** = determined by the Coordination Unit for Threat Analysis (CUTA)
Areas where there is a critical infrastructure particularly sensitive areas	Identification & Traffic data	**As of 2027** 6, 9 or 12 months, determined per zone by minister

Federal Police

What were the key issues ?

Federale Politie
Police Fédérale

What were the issues ?

1. Encryption
2. Definition of service provider
3. Technical difficulties on the side of the service providers
4. Type of data

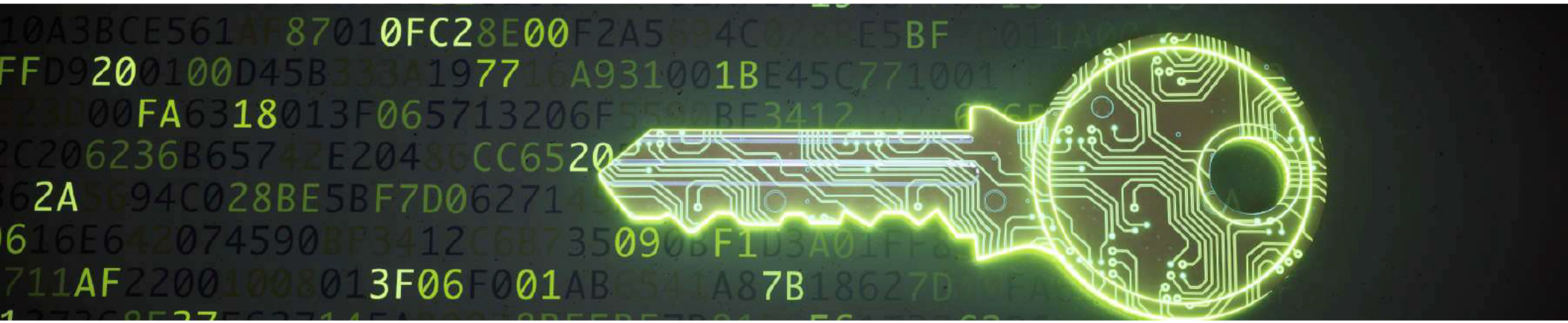
Federal Police

Importance of encryption in data retention

Federale Politie
Police Fédérale

Regading encryption

If the data retained by operators is incomprehensible to law enforcement, then the "Data Retention Act" is ...



An empty box

Principles of the law

Federale Politie
Police Fédérale

Principles of the law

1. There is no ban on encryption
   - It is even desired to promote digital security and security by design
2. However, there are (4) limits for operators

Federal Police

Limits for operators

1. Encryption cannot prevent emergency calls.
2. It cannot prevent the operator from meeting its data retention obligations.
3. It cannot render lawful interception impossible.
4. Any contractual clause which impedes a judicial investigation is prohibited and null and void (roaming, volte, Voice over Wifi, 5G)

→ Didn't solve the End-2-End encryption for interception.

→ Concept of the "front door" – Interception only for the future - – still an ongoing discussion. We don't want a back-door, wel a front door

→ WE DON'T BELIEVE THAT WE CAN WIN A TECHNICAL RACE WITH THE TECH Cie.

Federal Police

Providers

Definition of the provider

Person or enterprise providing electronic communications network or electronic communications service, available to the Belgian public… independently where the cie is situated

Federal Police

9

Data to be retained

Federale Politie
Police Fédérale

New data

- Identifier 5G (Succi –Supi)
- IP address
- MAC address
- Telephone on/off
- Jump between antenna during a data session

Federal Police

10

What’s next ?

Federale Politie
Police Fédérale

… Royal decrees to be prepared

- → 19 royal decrees in total
  (50 % are already prepared)
- → Preparing the implementation with the new actors (e.g. car manufacturer)

11

Conclusions

Federale Politie
Police Fédérale

Conclusions

- LEA : Let's hear our voice

  Bring the argument to rebalance the debate (not only a matter of Justice and National security)

- Rebalance the debate between LEA and the Big tech cie.
  Join our forces together : the companies have to collaborate (OBLIGATION) and we have to succeed in E-evidence / CSA / DSA …
  Keep our capacities « to attack » « dark platform/criminal operators »

- We have to think about a real technical collaboration at EU level (given the volume of data)

- What about an harmonized EU Data retention regime.

- We have to solve the « roaming » « end-2-end encryption ».

Federal Police

12

Questions ?

Federale Politie
Police Fédérale